CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1-40.
- After this Amendment: Claims 1-3, 6-10, 13-43

Non-Elected, Canceled, or Withdrawn claims: 4, 5, 11, 12

Amended claims: 1

New claims: 41-43

Claims:

1. (Currently Amended) A method comprising:

establishing at least one cryptography service parameter threshold comprising a minimum level of security;

selectively detecting a request for at least one cryptography service; and

selectively performing at least one correctness detection action based on ~~said~~ the requested cryptography service and ~~said~~ the at least one cryptography service parameter threshold, wherein;

the at least one correctness detection action selectively performed includes suggesting at least one alternative cryptography service~~, wherein~~ ;

the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and

the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length.

2. (Original) The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying unacceptable cryptography algorithms.

3. (Original) The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying acceptable cryptography algorithms.

4. (Canceled)

5. (Canceled)

6. **(Original)** The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier.

7. **(Original)** The method as recited in Claim 6, wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories comprising authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms.

8. **(Original)** The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying at least one acceptable seed size parameter.

9. **(Original)** The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying at least one unacceptable seed size parameter.

10. **(Original)** The method as recited in Claim 1, wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating

system, a cryptography system service, and another process calling into the cryptography application programming interfaces.

11. (Canceled)

12. (Canceled)

13. (Original) The method as recited in Claim 1, wherein selectively performing at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

14. (Original) The method as recited in Claim 13, wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

15. (Previously Presented) The method as recited in Claim 1, wherein selectively performing at least one correctness detection action based on said requested

cryptography service and said at least one cryptography service parameter threshold includes performing at least one action of a plurality of actions, the plurality of actions comprising:

interrupting at least one process;

stopping at least one process;

starting at least one process;

displaying alert information;

logging alert information;

suggesting at least one alternative cryptography service;

outputting alert messages;

causing alteration of a graphical user interface; and

forcing use of at least one other cryptography service.

16. (Previously Presented) A computer readable medium having computer-implementable instructions embodied thereon, which when executed cause one or more processing units to perform acts comprising:

establishing at least one cryptography service parameter threshold comprising a minimum cryptography service parameter threshold;

selectively detecting a request for at least one cryptography service; and

selectively performing at least one correctness detection action based on said requested cryptography service and said at least one minimum cryptography service

parameter threshold, wherein the at least one correctness detection action selectively performed includes forcing use of at least one alternative cryptography service.

17. (Previously Presented) The computer readable medium as recited in Claim 16, further comprising:

establishing at least one maximum cryptography service parameter threshold.

18. (Previously Presented) The computer readable medium as recited in Claim 17, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying unacceptable cryptography algorithms; and

identifying acceptable cryptography algorithms.

19. (Previously Presented) The computer readable medium as recited in Claim 17, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying at least one unacceptable cryptography key size parameter; and

identifying at least one acceptable cryptography key size parameter.

20. (Previously Presented) The computer readable medium as recited in Claim 17, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes establishing a plurality of correctness

categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier.

21. (Original) The computer readable medium as recited in Claim 20, wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories comprising authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms.

22. (Previously Presented) The computer readable medium as recited in Claim 17, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying at least one acceptable seed size parameter; and

identifying at least one unacceptable seed size parameter.

23. (Original) The computer readable medium as recited in Claim 16, wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface.

24. (Original) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on

said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

25. (Original) The computer readable medium as recited in Claim 24, wherein determining if said cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold includes comparing a size of said cryptographic key with said at least one cryptography service parameter threshold.

26. (Original) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

27. (Original) The computer readable medium as recited in Claim 26, wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service

parameter threshold further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

28. (Previously Presented) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes performing at least one action selected from a group of actions comprising interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, and causing alteration of a graphical user interface.

29. (Previously Presented) An apparatus comprising:

a system memory;

a processing unit; and

cryptography correctness detection logic configured to:

establish at least one cryptography service parameter threshold, wherein the at least one cryptography service parameter threshold comprises a threshold setting a minimum level of security;

selectively detect a request for at least one cryptography service; and

selectively perform at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not

satisfy the at least one cryptography service parameter threshold, wherein the at least one correctness detection action selectively performed includes forcing use of at least one other cryptography service, wherein the at least one other cryptography service comprises a cryptography service having a higher level of security than represented by the cryptography service parameter threshold.

30. (Original) The apparatus as recited in Claim 29, further comprising:

memory operatively coupled to said cryptography correctness detection logic; and

wherein said cryptography correctness detection logic is further configured to maintain said at least one cryptography service parameter threshold in said memory.

31. (Original) The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least one of the following: at least one unacceptable cryptography algorithm, and at least one acceptable cryptography algorithm.

32. (Original) The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least one of the following: at least one unacceptable cryptography key size parameter; and at least one acceptable cryptography key size parameter.

33. (Original) The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to establish a plurality of correctness categories in said memory, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier.

34. (Original) The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least one of the following:

at least one acceptable seed size parameter; and

at least one unacceptable seed size parameter.

35. (Original) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to monitor at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface.

36. (Original) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to determine if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

37. (Original) The apparatus as recited in Claim 36, wherein said cryptography correctness detection logic is further configured to compare a size of said cryptographic key with said at least one cryptography service parameter threshold.

38. (Original) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to determine if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

39. (Original) The apparatus as recited in Claim 38, wherein said cryptography correctness detection logic is further configured to compare a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

40. (Previously Presented) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to use at least one action selected from a group of actions comprising interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, and causing alteration of a graphical user interface, to be performed.

41. (New) The method as recited in Claim 1, wherein:

in an event that the cryptography service is an asymmetric cryptography service, the minimum level of security comprises a minimum acceptable public key size of at least 1024 bits; and

in an event that the cryptography service is a symmetric cryptography service, the minimum level of security comprises a minimum acceptable symmetric key size of at least 128 bits.

42. (New) The computer readable medium as recited in Claim 16, wherein:

the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and

the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length.

43. (New) The apparatus of claim 29 wherein the selectively performing at least one correctness detection action based on the requested cryptography service and

the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length.